

# U.S. Army Materiel Command



## Force Protection

“...To protect personnel, information,  
and critical resources....”

# Force Protection



## Table of Contents

|                                     | <u>Page</u> |
|-------------------------------------|-------------|
| Message from the Commanding General | 3           |
| U.S. Army Force Protection Program  | 5           |
| Traditional Terrorist Threat        | 6           |
| Terrorism Today                     | 8           |
| Terrorist Profile                   | 10          |
| Threat to Information Systems       | 14          |
| Electronic Terrorist Threat         | 16          |
| Information Systems Vulnerabilities | 18          |
| AMC Force Protection Program        | 20          |
| Individual Responsibilities         | 21          |
| AMC Commander's FP Imperatives      | 24          |
| Summary                             | 26          |
| THREATCON Levels                    | 27          |
| Training Requirements               | 28          |
| Force Protection Contacts           | 31          |
| AT/FP References                    | 32          |
| AT/FP Related Internet Websites     | 33          |

# *Message from the Commanding General*



Antiterrorism/Force Protection (AT/FP) is my most important priority. It is essential that each member of the Command treat Antiterrorism/Force Protection with the same degree of significance and attention.

The Army Materiel Command (AMC) has been the object in the recent past of various threats and attacks. The most serious incident at an AMC facility was the terrorist bombing at the Office of the Program Manager, Saudi Arabian National Guard in Riyadh, Saudi Arabia, on 13 November 1995. The explosion caused seven deaths, including five AMC members, and over sixty wounded.

Our global presence mandates extraordinary force protection measures to minimize exposure of personnel and equipment as targets for terrorist activities. Likewise, our dependence on information technology to accomplish the mission creates ever-increasing opportunities for terrorists to conduct low-risk, high-gain attacks on AMC information systems. In view of these potential threats and our recognized vulnerabilities, the question is not if we will experience an attack, but rather when and where.

As the U.S. Department of Defense faces new challenges in peacekeeping and humanitarian operations, the number of individuals and groups opposed to the United States increases. Weaker adversaries, who would not consider confronting the U.S. military with direct force, will turn to terrorism or other means to advance their cause.

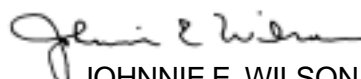
Our efforts to identify and apply Force Protection technology place AMC in a principal position in the security of Defense personnel, critical resources, and information. Elements of the Communications and Electronics Command are leading the Army in information assurance technologies. The Product Manager-Physical Security Equipment and the Quick Response Office are applying technology successfully to reduce terrorism risks to U.S. forces, most notably in Bosnia and Southwest Asia.

We should continue to interject this spirit of AT/FP innovation in all of our plans, operations, and activities. Force Protection impacts everyone from technology development in our laboratories, to testing, to acquisition, and to logistics power projection.

Antiterrorism/Force Protection is a leadership responsibility at each level in the AMC chain of command. Commanders and supervisors at all levels are responsible for implementing the AMC AT/FP Program and must be proactive. All leaders will study the contents of this booklet carefully, understand its imperatives, and take appropriate steps to implement them.

Equally important is that all members of the Command support the Antiterrorism/Force Protection Program and do their part to ensure success. The lives of our soldiers, civilians and family members are too precious for us to place them at risk by doing anything less than our best to protect them.

The U.S. Army Materiel Command – America's Arsenal for the Brave.

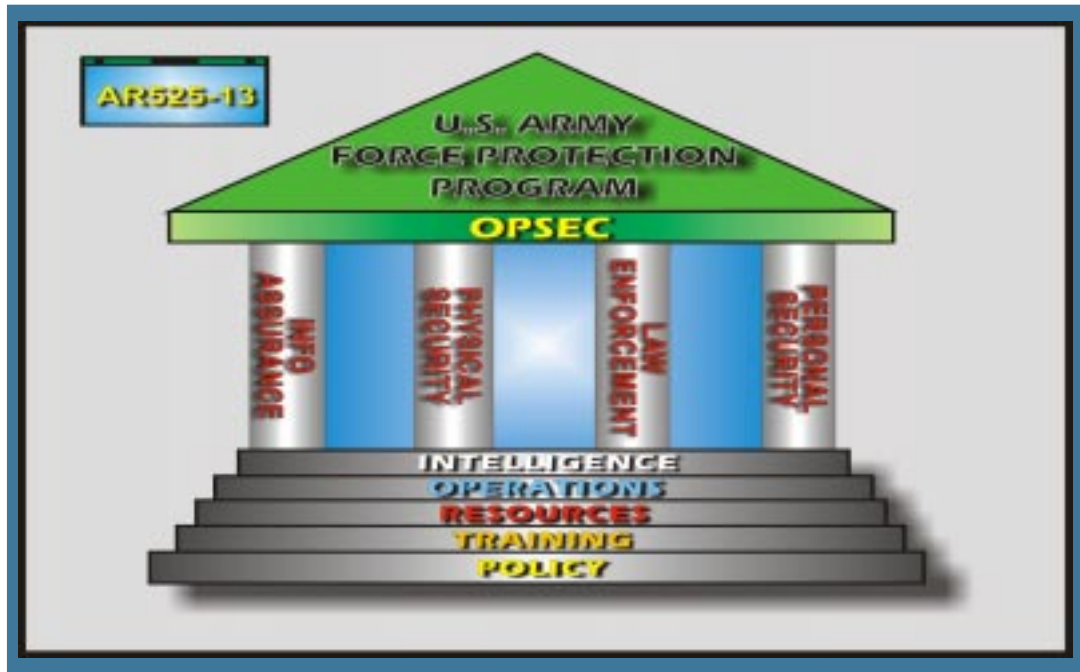
  
JOHNNIE E. WILSON  
General, USA  
Commanding





# *The Army Force Protection Program*

The Army defines its Antiterrorism Force Protection Program in the Antiterrorism Force Protection (AT/FP): Security of Personnel, Information, and Critical Resources, AR 525-13, as: "A security program to protect personnel, information, and critical resources from asymmetrical attacks. This is accomplished through the planned integration of personal security, the protection of command and control capabilities (C2 Protect), physical security, and law enforcement, all supported by the synchronization of doctrine, training, operations, intelligence, and resources."



**AMC must continuously synchronize the core security components of the AT/FP program. These components are described below:**

**Physical Security Measures:** Designed to deter, detect, and defend U.S. Forces and materials from: terrorist, criminals, disaffected persons, hostile intelligence, paramilitary forces, protesters, and saboteurs.

**Information Assurance:** Information Assurance (C2 Protect) is a function of Information Operations that protects the force by maintaining effective C2 of friendly forces and negating or turning to friendly advantage the adversary's efforts to influence, degrade, or destroy friendly C2 systems.

**Personal Security:** Personal Security measures range from institutional training and general individual counter measures, to specialized protective services.

**Law Enforcement:** Assists in Force Protection through prevention, detection, response and investigation of crime.

**Operations Security (OPSEC):** The goal of OPSEC is to control information and observable actions about friendly force capabilities, limitations, and intentions so as to prevent or control their exploitation by an adversary.



**"...The threat to US interests and citizens worldwide remains high. ...US citizens and facilities suffered more than 30 percent of the total number of terrorist attacks in 1997 - up from 25 percent last year."**

**George J. Tenet  
Director of Central Intelligence  
January 28, 1998**







# *The Traditional Terrorist Threat*

## What is terrorism?

The Army defines terrorism in AR 525-13 as: “The calculated use of violence or threat of violence to inculcate fear; intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological.”

Terrorism has been with us throughout history. Usually directed against innocents, it is a tactic by which those without political power hope to influence governments and societies. The goal has always been to generate fear, horror, and disgust so that giving in to terrorist demands becomes acceptable to the general public. These terrorist actions undercut the legitimacy of the government by demonstrating that it is unable to protect its citizens. Simply put, the weak are able to influence the strong. The public then demands changes to government policies that would satisfy the political, religious, or ideological demands of the terrorists.

An upsurge in terrorism in the late 1960's, particularly in the Middle East and Western Europe, had the opposite effect. Governments refused to give in to terrorist's demands and developed expertise in targeting and eliminating terrorist organizations. Protection against

the terrorist threat was understood to require offensive counter-terrorism (CT) and defensive antiterrorism (AT) capabilities and programs.

The combined success of CT and the break up of the Soviet Union forced terrorists to change their tactics. Previously, hijackings and hostage taking had been the favored method of attack; but as CT expertise increased and safe-havens disappeared, terrorists resorted to bombings and assassinations to limit their exposure to CT forces. Simultaneously, terrorist expertise increased significantly in operations security (OPSEC), intelligence gathering, and planning. As terrorists minimize exposure to counter-terrorism forces, the relative importance of terrorism increases.

Whereas counter-terrorism requires special expertise and extensive training of elite units, basic antiterrorism measures can be learned and implemented by virtually anyone.



Today we are faced with the real and growing threat of terrorism in the United States. The Army Materiel Command spans the globe and must maintain constant vigilance against the terrorist threat both in the United States and its many facilities abroad. There are a number of real world threats to AMC personnel, family members, facilities & information systems, threats that we all face to one extent or another on a daily basis.

## International Terrorism

International terrorism involves the planning or execution of a terrorist act that crosses national boundaries. The FBI defines international terrorism as terrorist activity involving groups or individuals whose activities are foreign based and/or directed by countries or groups outside the United States or groups or activities whose activities transcend national boundaries. These types of acts are usually planned to attract widespread publicity and are designed to focus attention on the existence, cause or demand of the terrorists.

## Domestic Terrorism

The FBI defines domestic terrorism as terrorist activity without foreign direction involving groups or individuals whose activities are directed at elements of our government or population. This is terrorism perpetrated by the citizens of one country against fellow countrymen and includes acts against citizens of a second country when they are in the host country, and not the principal or intended target.

### **U.S. Policy on Terrorism**

**It is the policy of the United States to deter, defeat and respond vigorously to all terrorist attacks on our territory and against our citizens, or facilities, whether they occur domestically, in international waters or airspace or on foreign territory. The United States regards all such terrorism as a potential threat to national security as well as a criminal act and will apply all appropriate means to combat it.**

**Presidential Decision Directive 39  
June 21, 1995**

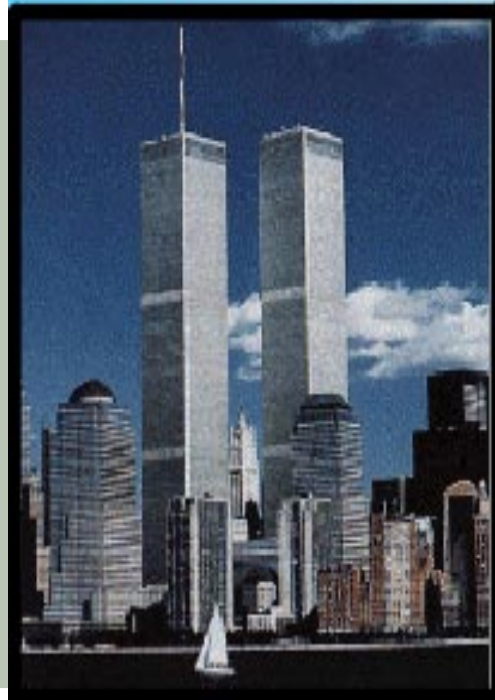




# ***Terrorism Today***

We live in a world where terrorism is becoming a fact of life. Four recent examples of terrorist acts bring to the forefront the magnitude of the terrorist threat facing the United States. This is of special concern to military personnel and federal employees:

The bombing of the World Trade Center on 26 February 1993, killed 6 US citizens and injured hundreds more. This was the first major terrorist attack that occurred on US soil. It brought domestic terrorism to the forefront of American public thought and created a new interest in the study of terrorism and in combating terrorist activities. This attack was directly linked to an Egyptian terrorist group. Its leader Shaykh Abdel Rahman, was later arrested, tried and convicted of conspiring to commit terrorist acts within the US.



## ***In America...***

The bombing of the Alfred P. Murrah Federal Building in Oklahoma City, Oklahoma on 19 April 1995, killed 168 US citizens and injured hundreds more. Timothy McVeigh was convicted of the bombing and was sentenced to death. His accomplice, Terry Nichols, was convicted of conspiracy and eight counts of involuntary manslaughter. The Oklahoma City bombing demonstrates that

foreign interests are not always at the root of terrorism.





**"Force Protection is an inherent command responsibility and must be fully integrated into every unit's mission."**

**General Dennis Reimer  
Chief of Staff, U.S. Army  
November 1, 1996**

At 11:33 AM, 13 November 1995, terrorists exploded a bomb in a pick-up truck in the parking lot of the Of-



ice of the Program Manager, Saudi Arabian National Guard (PM-SANG), Riyadh, Saudi Arabia. PM-SANG is an Army Materiel Command organization that is subordinate to the Commander, U.S. Army Security Assistance Command. The explosion killed seven people, including one U.S. Army Noncommissioned Officer, four Department of the Army Civilians, and two In-

dian nationals, and wounded over 60 others. A joint Saudi-FBI investigation resulted in the arrest, conviction and execution of four Saudi nationals.

## *...and Overseas*

The Khobar Towers bombing in Dhahran, Saudi Arabia, 25 June 1996, killed 19 Americans and injured over 500 Americans. It was an example of international terrorism. The location was specifically targeted to shock the American public and to reduce US effectiveness in the region.





# *The Terrorist Profile*

The Defense Intelligence Agency (DIA) estimates that more than 15 foreign terrorists groups have both the ability and motivation to operate in the United States. The attack on the World Trade Center in 1993, by an organization loosely affiliated with an Islamic Group based in Egypt was the most dramatic example of international terrorism perpetrated here. Recent incidents of letter bombs originating from Egypt demonstrate that foreign terrorists will continue to launch attacks on our country. Well known international groups such as Hamas, Hizballah, and the Palestine Islamic Jihad continue to express their opposition to the United States and retain the ability to strike with little warning.



Americans have little sympathy for terrorists. Terrorist groups, like those based in the Mid-East, are virtually non-existent in the United States. What does exist is a diverse array of extremist organizations, which officially do not condone terrorism but may serve as breeding grounds for terrorist activities.

Most terrorist incidents in the United States involve individuals or small extremist groups that strike once and are then quickly apprehended. A lack of popular support for terrorism and efficient law enforcement limits the number of repeat offenders. Unfortunately, most terrorists' attacks are instigated by little-known, first-time assailants, acting independently for personal reasons or as a result of some form of mental instability.



## **Extremist groups are organizations that—**

- \* **Espouse racial supremacy causes.**
- \* **Foster discrimination based on race, creed, color, gender, religion, or national origin.**
- \* **Advocate the use of force or violence, or otherwise engage in efforts to deprive individuals of their civil rights.**



**“...Terrorism is a worldwide phenomenon. No nation is immune: certainly not the United States - where terrorists have struck from lower Manhattan to Oklahoma city.”**

**Madeline K. Albright  
Secretary of State  
October 8, 1997**

Domestic organizations range from organized militias to “single-issue” groups espousing specific causes. Although most individuals within these organizations live within the law, the common ingredients of terrorism—such as zealotry for a particular cause or belief, dissatisfaction with the US Government, and



weapons skills or intelligence skills are often present. According to unofficial estimates, these so called “patriotic” organizations may number more than 800. Among the more than 200 militias in the United States, it is estimated that more than 40 may be armed. However, our nation’s protection of personal liberties and constitutional rights precludes taking arbitrary legal measures against groups or individuals based solely on profiles or personal beliefs that are legally expressed.

## ***Terrorist - Typical Characteristics***

Despite the wide array of personal beliefs and backgrounds, terrorists have several key similarities that can lay the groundwork for understanding and dealing with the problem. According to key intelligence sources, terrorists are typically “intelligent, well-educated, obsessed with initiating a change in the status quo, reared in middle-class or affluent families, 22 to 25 years of age, and motivated by religion, prestige, power, political change, or material gain.”





Many terrorists have also lived on the fringes of extremist organizations and have had prior encounters with law enforcement agencies. They operate in a murky world where extremism, terrorism, and “common” criminal activities frequently cross. They are often known to law enforcement agencies, even if not immediately identifiable as terrorists.



The terrorist weapon of choice is the bomb. Most terrorists operating in the United States recognize that other forms of terrorism, such as kidnappings and hijackings, will seldom achieve the desired effects and usually result in their immediate capture. A bomb provides the safety of distance and an immediate, dramatic impact.



## The future of terrorism may follow any of several disturbing trends.

The nerve agent attacks in Japan's subway system alerted us to the relative ease with which a terrorist can obtain and employ weapons of mass destruction and to the vulnerability of public transportation. Several studies have cited the difficulty of accounting for and controlling of nuclear materials both refined and by product, generated by the former Soviet Union. Though constructing a nuclear device requires precise, sophisticated technology, spreading nuclear contamination does not. A member of a domestic hate group reportedly was arrested for illegally attempting to obtain bubonic plague virus by mail. Increasingly frequent and sophisticated intrusions into our nation's computer networks have sensitized us to the potential threat of cyberterrorism.

Though we cannot be certain which of these paths tomorrow's terrorists will take; the AT/FP program fundamentals we establish now will be equally effective against the future threat.





# *The Information Systems Threat*

## Hackers.....



The electronic threat to Department of Defense activities in general and AMC in particular are not limited to foreign or domestic terrorists. The same systems are vulnerable to the careless efforts of inquisitive hackers, the interests of criminals and organized crime and the vagaries of nature.

Hackers attempt to penetrate systems for a number of reasons. Among these are curiosity, personal gain and the challenge of overcoming security barriers. However, the impact on the information systems from hacking is the same regardless of the motivations of the hackers. Unauthorized people gain access to information critical to our mission and may be tempted to interrupt the flow of that



information, share it with others, or change it by accident or for personal enjoyment. In either case, the interruption of the flow of information can have a critical effect on our ability to do our jobs.

"...we have identified several countries that have government-sponsored information warfare programs underway. It's clear that those developing these programs recognize the value of attacking a country's computer systems - both on the battlefield and in the civilian arena. In addition, I believe terrorist groups and other non-state actors will increasingly view information systems in the United States as a target."

George J. Tenet  
Director of Central Intelligence  
January 28, 1998





## .....Criminals and Nature

Individual criminals and organized crime are motivated by profit to break into government systems to steal potentially useful materials or information for eventual sale. The impact of these intrusions is the same as that for the hackers: potentially disrupted information flow, unauthorized access to sensitive information, the possible compromise of sensitive information, and the potential unauthorized modification of critical data.



Nature has, and will continue to impact, human systems. Floods shut down the Chicago financial district in the 1980's, hurricanes have shut down the operation of entire communities in Florida and along the East Coast, and earthquakes have stopped commercial and government activities in Southern California. While none of this directly relates to terrorist activities, the effects of these natural disasters on our ability to accomplish our mission is the same. As a result, we have to make plans to continue our operations in the face of terrorist disruptions as well as natural disasters.



# ***The Electronic Terrorist Threat***

In 1990, President Bush issued National Security Directive 42, portions of which were declassified on April 1, 1992. This directive recognized the vulnerability to national telecommunications and information processing systems. The directive calls them “highly susceptible to interception, unauthorized access, and related forms of technical exploitations as well as other dimensions of the foreign intelligence threat.” The directive also notes that “the technology to exploit these electronic systems is widespread and is used extensively by foreign nations and can be employed, as well, by terrorists groups and criminal elements.”

In June 1996 the U.S. Senate Government Affairs Committee Permanent Committee on Investigations released the Minority Staff Report, Security in Cyberspace, that called for swift attention to the defense of our National Information Infrastructure (NII).

On June 25, 1996, former Director of Central Intelligence (DCI) John Deutch testified before this committee warning that the country will face some “very large and uncomfortable” incidents at the hands of foreign computer terrorists. Deutch testified that these information attacks could not only “disrupt our daily lives, but also seriously jeopardize our national or economic security.” Deutch also noted that “virtually any ‘bad actor’ can acquire the hardware and software needed to attack some of our critical information-based infrastructures.”



## **GROUP CLAIMS HIGH ACCESS TO US MILITARY NETWORKS**

By James Glave  
21 April 1998

**San Francisco, CA (Wired) - In what may be one of the first demonstrations of the potential of cyber warfare, an international hacking group claims it has stolen a suite of programs used to run classified US military networks and satellites.**



***In response to PDD 39***, the Attorney General established the Critical Infrastructure Working Group, which included representatives from the Department of Defense and the intelligence community. The group identified eight national critical infrastructures: telecommunications, transportation, emergency services, banking and finance, electrical power systems, water supply systems, gas/oil storage and transportation, and continuity of government. The group also identified two categories of threat to these infrastructures -- physical and cyber.

## **President Clinton on Cyber Attacks**

"As we approach the 21st century, our foes have extended the fields of battle from physical space to cyberspace, from the world's vast bodies of water to the complex workings of our own human body. Rather than invading our beaches or launching bombers, these adversaries may attempt cyber attacks against our critical military systems and our economic base."

President Clinton  
Address at U.S. Naval Academy  
May 22, 1998

***Information Operations (FM 100-6):*** Information Operations (IO) integrate all aspects of information to support and enhance the elements of combat power, with the goal of dominating the battlespace at the right time, at the right place, and with the right weapons or resources. IO are defined as continuous military operations within the Military Information Environment (MIE) that enable, enhance, and protect the friendly force's ability to collect, process, and act on information to achieve an advantage across the full range of military operations. IO includes interacting with the Global Information Environment (GIE) and exploiting or denying an adversary's information and decision capabilities. Units conduct IO across the full range of military operations, from operations in garrison, through deployment, to combat operations, and continuing through redeployment upon mission completion.





# Information Systems Vulnerabilities

In 1996, the US Congress requested that the General Accounting Office (GAO) review the extent to which Department of Defense (DOD) computer systems are attacked. The review was to focus on the potential for further damage to DOD computer systems, and the challenges DOD faces in securing sensitive information on it's computer systems. This GAO review produced a report to Congress, Information Security: Computer Attacks at Department of Defense Pose Increasing Risks (Chapter Report, 05/22/96).

- \* DOD relies on a complex information infrastructure to design weapons, identify and track enemy targets, pay soldiers, mobilize reservists, and manage supplies;
- \* Use of the Internet to enhance communication and information sharing has increased DOD exposure to attack, since the Internet provides unauthorized users a means to access DOD systems;
- \* While DOD information available on the Internet is unclassified, it is sensitive and must be restricted;
- \* Only about 1 in 500 attacks is detected and reported, but the Defense Information Systems Agency (DISA) estimates that DOD is attacked about 250,000 times per year;
- \* Attackers have stolen, modified, and destroyed data and software, disabled protection systems to allow future unauthorized access, and shut down entire systems and networks to preclude authorized use;
- \* Security breaches pose a serious risk to national security because terrorists or other U.S. adversaries could disrupt the national information infrastructure;
- \* Security breaches cost DOD hundreds of millions of dollars annually;
- \* DOD needs to increase the resources devoted to computer security, update the policies that govern computer security, and increase security training for system and network administrators.





The GAO review also found that there is mounting evidence that attacks on DOD computer systems pose a serious threat to national security. Internet connections make it possible for enemies armed with less equipment and fewer weapons to gain a competitive edge at a small price.

As a result, this will become an increasingly attractive way for terrorist or adversaries to wage attacks against DOD. For example, major disruptions to military operations and readiness could threaten national security if attackers successfully corrupt sensitive information and systems or deny service from vital communications backbones or power systems.

## SPY AGENCY TO PROBE NASA COMPUTER SECURITY

11 May 1998

Defense Week

By John Donnelly

**Teams from the National Security Agency will soon try to break into unclassified computer networks at NASA to determine how robust the space agency is at fending off cyber-intruders who could threaten satellite control, launch control and other critical operations.**

The National Security Agency has acknowledged that potential adversaries are developing a body of knowledge about Defense and other national systems and are creating methods to attack these systems. According to DOD officials, these methods, which include sophisticated computer viruses and automated attack routines, allow adversaries to launch untraceable attacks from anywhere in the world. In some extreme scenarios, studies show that terrorists or other adversaries could seize control of DOD information systems and seriously degrade the nation's ability to deploy and sustain military forces. Official estimates show that more than 120 countries already have or are developing such computer attack capabilities.

## CYBERTERRORISM

*"Cyberterrorism will occur where we are most vulnerable: where we are reliant and dependent on systems that exist at the convergence of the physical and virtual worlds. Where cracking means more than changing a webpage; it means damage, injury and potential lethality."*

Barry C. Colin  
The Institute for Security and Intelligence  
Stanford, CA  
November 19, 1997



# ***The AMC Force Protection Program***

The AMC Antiterrorism/Force Protection program serves two primary purposes. First, it provides the framework for the protection of our people, our most important resource. Second, and equally important, it serves as our contribution to the Army's readiness. It contributes to the protection of critical stockpiles of weapons, munitions, and other essential equipment entrusted to our Command. It is this aspect that makes the AMC Antiterrorism/Force Protection Program unique from others in the Army.

Force Protection is a systemic program with "dynamic" emphasis. Our intent must be to incorporate force protection measures as a routine into all operations—tactical, logistical and administrative.

The technical nature of AMC's mission requires an extreme dependence on information systems and networks. The electronic infrastructure, both public and private, that makes our electronic communications possible forms an essential backbone for operations. AMC mission capabilities could be severely degraded by the loss of any portion of the electronic infrastructure or the failure of any critical AMC information system, network, or information storage device. The threat to AMC personnel and equipment, both in CONUS and OCONUS, is real. AMC's global presence and mission on behalf of the United States exposes personnel and equipment as potential targets to criminal, terrorist, and zealot actions. Protecting organizational equities at home and abroad mandates the need for a comprehensive Antiterrorism/Force Protection (AT/FP) Program which is easily understood and implemented by all AMC military, civilian, and contractor personnel.

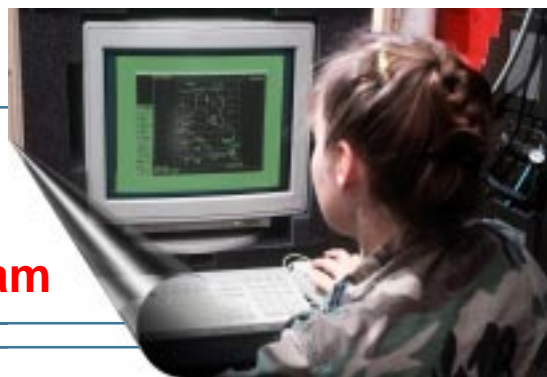
## ***Key AMC Policy Documents***

### **AMC Regulation 525-13**

## **The AMC Force Protection Program**

### **AMC Circular 525-1**

## **AMC Force Protection Management Structure**





# Individual Responsibilities



## Recognize the Threat

**The key to threat recognition** is the ability to recognize when something is out of place. This also includes criminal, personal and other threats. No terrorist incident occurs



without considerable planning and pre-mission reconnaissance by the terrorists. Terrorists can be vulnerable to discovery while they are conducting target reconnaissance because they often fail to blend in to their surroundings. Terrorist's reconnaissance activities, such as taking photographs, making sketches, note taking, or displaying unusual interest in AMC activities or facilities may provide vital early warning - but only if it is recognized and reported. Differences in culture may also cause terrorists to unknowingly act or dress in ways that are inappropriate for their surroundings. Be observant; notice the out-of-place or unusual activity and pay attention to your surroundings.

Recognizing unusual events includes developing a heightened awareness of the electronic threat. When someone calls and claims to have a good reason for asking for passwords, modem phone numbers, or other sensitive information they may be trying to trick you into revealing information that could compromise the security of AMC computers and networks. This kind of approach is called "social engineering" and it is often successful because most people want to be helpful and they do not want to be perceived as being overly suspicious. Your "helpful" response to a social engineering inquiry could provide an attacker with electronic keys to AMC's cyber-defenses.





## Report Suspicious Activities

Every AMC soldier or employee has the ability to support counter terrorism by recognizing suspicious activities and electronic incidents. Become intimately familiar with individual protective measures. They can be found in GTA 19-4-3 (Jul 97) and JS Guide 5260.

Recognizing that something is out of place is only the first step. The second step is to report the suspicious activity or incident to the proper authorities. Reporting a suspicious activity or incident that later turns out to have a reasonable explanation is always preferable to ignoring it.



Reportable activities and incidents are many and varied. If you believe that someone is trying to collect sensitive information about AMC information systems, immediately report it to your chain of command. Other examples of reportable incidents include: computer virus infections (even if they are stopped by anti-virus software); any modem activity that you did not initiate; any unexplained file additions, deletions, or modifications; any suspicious unsolicited e-mail correspondence; and, any computer or network related incident that prevents you from supporting the AMC mission.

**New and unique vulnerabilities occur frequently when performing your mission. If you observe a vulnerability, report it as you would suspicious activity.**



## CYBER Protection

Attacks on computer systems are a serious and growing problem. The potential for catastrophic damage is great. Organized foreign nationals or terrorists could use "information warfare" techniques to disrupt military operations by harming command and control systems, logistics databases or networks used to transmit data.

**Every individual will ensure that first line protective measures are adhered to as part of AMC's AT/FP Program. The following are the required first line protective measures to be taken:**

- \* Protect your monitor screen and printer output from unauthorized access by individuals.
- \* Protect your password.
- \* Be alert to possible network intrusions, database tampering, and security incidents.
- \* Protect against computer viruses by using a virus scan program on all PC's.
- \* Know how and where to report possible network intrusion or tampering.
- \* Report security incidents to your Information Systems Security Officer and Systems Administrator.
- \* If there is any question about possible tampering with your systems, call the organization Help Desk for assistance.



### ***Report Information System Security Incidents***

The Army Computer Emergency Response Team (ARECT) is chartered to assist in investigating Information system's Security (ISS) incidents. Upon the discovery of an incident, the ACERT must be notified by telephone immediately and by written report within 24 hours. The ACERT toll-free telephone number is 1-888-203-6332, commercial is (703) 706-1113, and DSN is 235-1113. Non secure fax is commercial (703) 806-1152 and DSN 656-1152; secure fax is (703) 806-1004 and DSN 656-1004.

**"ALL INCIDENTS MUST BE REPORTED TO THIS ACTIVITY."**

AMCMI Memorandum  
Subject: Information System & Security Incident Reporting  
February 5, 1998





## AMC Commander's



*Each member of the command has individual responsibilities in support of the Force Protection Program. These individual responsibilities, known as the AMC Commander's Ten Force Protection Imperatives, are listed on this and the following page.*

**1. KNOW THE THREAT.** Be aware of the threats and our vulnerabilities to those threats.

**2. TAKE FORCE PROTECTION SERIOUSLY.** Read and understand this booklet on Force Protection; take the subject seriously. Discuss this information with your family members when appropriate. Include Force Protection as a consideration in all your activities.

**3. OBSERVE AND REPORT.** Notice things that are out of the ordinary and could be surveillance prior to a terrorist attack. Look for strangers paying particular attention to our activities. Report unusual incidents to the security, police, or law enforcement agency.

**4. GET LEVEL I AT/FP TRAINING BEFORE TRAVEL.** Prior to OCONUS travel and deployments, contact your organization's Antiterrorism Force Protection Officer to receive the mandatory individual AT/FP Level I briefing and handouts. This is to increase personal protection and to satisfy regulatory requirements.



# Force Protection Imperatives



**5. BE READY.** Always maintain an awareness of Antiterrorism Force Protection and be ready to increase your vigilance and individual protective measures as needed.

**6. OBEY AT/FP GUIDANCE.**

Follow U.S. Army and local command AT/FP guidance, including specific measures related to each THREATCON level. Cooperate with our security elements. Sometimes what they require is inconvenient in the short term, but the purpose of their actions is to keep us safe and operational.

**7. ENSURE EVERYONE IS AWARE.**

Talk to your co-workers and your families to ensure that they are aware of the threat and the measures they can take to minimize risks.



**8. BE UNPREDICTABLE.** Vary your routes and departure times between work and home.

**9. KNOW YOUR FORCE PROTECTION OFFICER.** Know the name of your organization's Force Protection Officer and how to contact that individual.

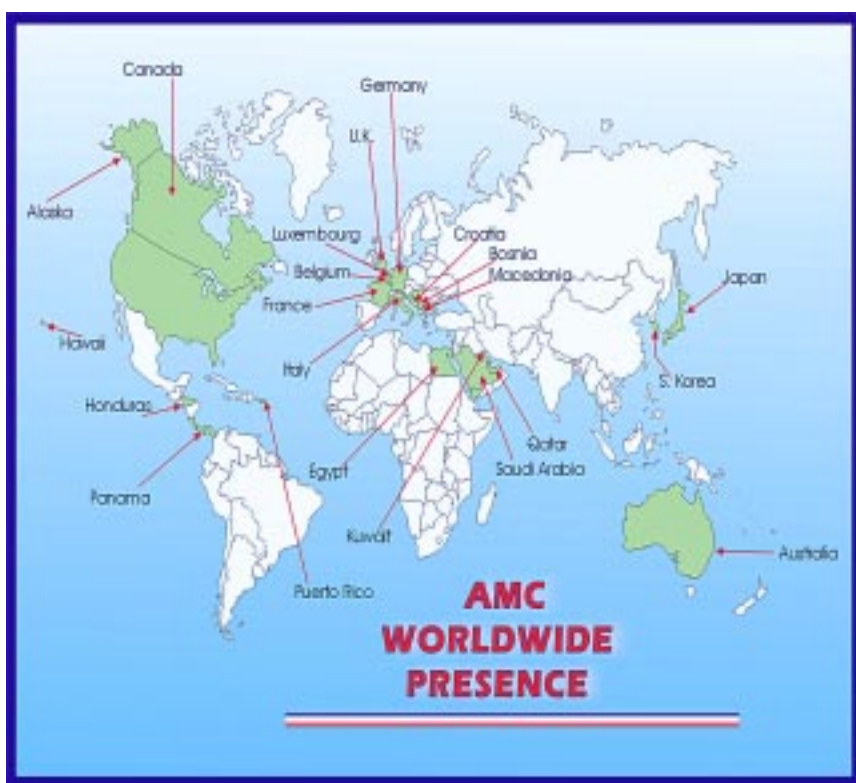
**10. KEEP A LOW PROFILE.** Your dress, conduct and mannerisms should not attract attention.



## Summary

There are real terrorist threats to the AMC family and they are not limited to foreign threats. Unfortunately, some of our own citizens have become so disenchanted with our system of government or so preoccupied with racial, ethnic or regional hatred that they now present a credible threat to both governmental activities and members of the AMC family. These threats have also changed the targets of their terrorism. Where once we could concern ourselves with the physical protection of our facilities and people, now we must also pay close attention to the protection of the electronic systems upon which we depend to process, store and communicate the information that supports our decisions and daily operations. Those very systems that allow us to communicate better and work more productively make us vulnerable to terrorist attacks.

The very nature of our business makes us more vulnerable to these terrorist threats than other government activities. The AMC family is scattered across the entire country with many activities located within the civilian community instead of on protected military facilities. Our people live and work in various communities, making them more vulnerable to surveillance, tracking and terrorist activities.



By better understanding the threat, our vulnerabilities to the threat, and by following a few simple steps to minimize our collective risks, we can all continue to provide the critical support to the warfighter that we have always provided in a safe and secure environment.





## ***THREATCON Levels***

**(1) THREATCON NORMAL** Applies when there is no discernible threat of possible terrorist activity. Under these conditions, only a routine security posture, designed to defeat the criminal threat, is warranted. The minimum THREATCON for U.S. Army commands is NORMAL.

**(2) THREATCON ALPHA** Applies when there is a general threat of possible terrorist activity against personnel and/or installations, the nature and extent of which is unpredictable, and circumstances do not justify implementation of THREATCON BRAVO measures. However, it may be necessary to implement certain measures from higher THREATCONS resulting from intelligence received or as a deterrent. Commands must be capable of maintaining THREATCON ALPHA measures indefinitely, with only limited impact on normal operations.

**(3) THREATCON BRAVO** Applies when an increased or more predictable threat of terrorist activity exists. Commanders must be capable of maintaining the measures of this THREATCON for several weeks without causing undue hardship to personnel or substantially affecting operational capabilities or aggravating relations with local authorities and members of the local civilian or host nation community.

**(4) THREATCON CHARLIE** Applies when an incident occurs or intelligence indicates that some form of terrorist action against personnel and/or facilities is imminent. Implementation of THREATCON CHARLIE measures for more than a short period probably will create hardships for personnel and affect the peacetime activities of units and personnel.

**(5) THREATCON DELTA** Implementation applies in the immediate area where a terrorist attack has occurred or when intelligence indicated that terrorist action against a specific location is likely. Implementation of THREATCON DELTA normally occurs for only limited periods of time over specific, localized area. Commands can not sustain THREATCON DELTA for extended periods without causing significant hardship for personnel and substantial reductions in capability to perform normal peacetime missions.



# Training Requirements

**Found in AR 525-13 and AMC Regulation. The local training program plus DoD required Antiterrorism Awareness Training requirements:**

## Level I-IV Training Requirements

| <u>Level of Training</u>                                    | <u>Target Audience</u>  | <u>Minimum Training Standard</u>  |
|---|---|---|
| <b>Level I</b><br><b>(Negligible/</b><br><b>Low Threat)</b> | Soldiers, DA Civilians, and family members deploying/traveling on government orders to Negligible or Low Terrorist Threat Level Areas | <ul style="list-style-type: none"> <li>* View AT Awareness Videos:               <ul style="list-style-type: none"> <li>- TVT 19-155 Intro to Terrorism</li> <li>- TVT 19-156 Terrorist Operations</li> <li>- TVT 19-157 Individual Protective Measures</li> </ul> </li> <li>* AT Awareness Handout:               <ul style="list-style-type: none"> <li>- JS Guide 5260; "Service Member's Personal Protection Guide: A Self-Help Handbook to Combating Terrorism" July 1996 or GTA 19-4-3; "Individual Protective Measures" July 1997.</li> </ul> </li> <li>* Recent AOR update for area travel</li> </ul> |
| Conducted<br>Within six<br>Months prior<br>to travel        |   |   |
| <b>Level I</b><br><b>(Medium/</b><br><b>High Threat)</b>    | Soldiers, DA Civilians, and family members' deploying/traveling on government orders to Medium or High Terrorist Threat Level Areas   | <ul style="list-style-type: none"> <li>* Same requirement as above, plus view AT Awareness Videos:               <ul style="list-style-type: none"> <li>-TVT 19-158 Surveillance Detection</li> <li>-TVT 19-159 Hostage Survival</li> </ul> </li> <li>* Instruction by qualified instructor using USAMPS developed lesson plans<br/> <i>Qualified Instructor = Level II qualified, or formal training in AT individual protection: O6 Commander or higher determines if qualified</i> </li> </ul>   |
| Conducted<br>Within 6<br>Months prior<br>to travel          |   |   |

### INDIVIDUAL TRAINING Army Standard 16 AR 525-13

***Commanders will ensure all military and DA Civilian personnel in their command receive appropriate individual antiterrorism awareness training prior to all travel and deployments outside the 50 United States, its territories and possessions.***



### Level of Training

### Target Audience

### Minimum Training Standard

Level II  
FP Officer

FP Officers who are then certified/current to serve as the Commander's FP Advisor and provide Level I instruction and training for hostage/kidnapping situations

\* Attend USAMPS's "The Force Protection Unit Advisor's Course"  
**Module A:** FP Level I Training  
 - Intro. to Terrorism (RJ1200)  
 - Terrorism Operations (RJ1205)  
 - Individual & Unit Protective Measures (RJ1215)  
 - Hostage Survival Techniques (RJ 1225)  
 - Terrorist Surveillance Detection (RJ1235)  
**Module B:** Force Protection Advisor Training  
 -Physical Security  
 -Information Management  
 -THREATCON  
 -Risk Management  
 -Bomb Threat Management & Improvised Explosive Devices  
 -Case studies

Level III

05-06 Commanders Program

\* "Implement the Army's Force Protection Program"  
 -Taught in branch PCCs & Garrison Pre-Command Course

Level IV

0-6 to 0-8 Commanders  
 Personnel who are responsible for FP programs or involved in FP policy planning and execution.

Executive level seminar providing pertinent AT/FP protection updates, briefings and panel discussions. Seminar will conclude with a tabletop FP wargame aimed at facilitating interaction and discussion among the participants.





# *Training Courses*



## **Courses That Certify Level I Instructors:**

- \* Force Protection Unit Advisor Course  
--U.S. Army Military Police School, Ft McClellan, AL
- \* Antiterrorism Instructor Qualification Course  
--U.S. Army JFKSW Center, Ft Bragg, NC

## **Other Force Protection Related Courses:**

- \* Individual Terrorism Awareness Course  
--U.S. Army JFKSW Center, Ft Bragg, NC
- \* Dynamics of International Terrorism Course  
--USAF Special Operations School, Hurlburt Field, FL
- \* Chemical/Biological Counterterrorism Course  
--U.S. Army Chemical School, Ft McClellan, AL
- \* Intelligence in Combating Terrorism  
--U.S. Army Intelligence Center and School, Ft Huachuca, AZ
- \* Counterterrorism Analysis Course  
--Joint Military Intelligence Center, Washington, D.C.



# Force Protection

## Contacts



### HEADQUARTERS, ARMY MATERIEL COMMAND (AMC)

COM (703) 617-0674    AFTER DUTY HOURS: 703-617-8612

DSN 767

AMCLG-OF

### AMC MAJOR SUBORDINATE COMMANDS:

#### Aviation and Missile Command

COM (205) 876-4105

DSN 746

AMSAM-PT-MO-SC

#### Army Research Laboratory

COM (301) 394-4558

AMSRL-CS-IO-SC

#### Chemical and Biological Defense Command

COM (410) 612-7248

DSN 548

AMCSB-OPR

#### Communications-Electronics Command

COM (732) 532-3105

DSN 992

AMSEL-PE-OC

#### Industrial Operations Command

COM (309) 782-1529

DSN 793

AMSIO-DMP

#### Soldier System Command

COM (508) 233-5062

DSN 256

AMSSC-SRE

#### Simulation, Training & Instrumentation Command

COM (409) 384-3540

DSN 970

AMSTI-CSS

COM (810) 574-5697

DSN 786

AMSTRA-RM-XM

#### Security Assistance Command

COM (703) 617-7016

DSN 767

AMSAC-SA

#### Test and Evaluation Command

COM (410) 278-1279

DSN 298

AMSTE-SM-I

#### Tank-Automotive & Armaments Command

COM (810) 574-5697

DSN 786

AMSTRA-RM-XM

### DoD FORCE PROTECTION POINTS OF CONTACT:

#### U.S. Army

COM (703) 695-8491

DSN 225

DAMO-FP

#### Defense Special Weapons Agency (FP Program Office)

Joint Service Integrated Vulnerability Assessments

COM (703) 325-7513

DSN 221

DSWA-PMF

#### Joint Staff (J-34)

COM (703) 693-7520

DSN 223



## KEY ANTITERRORISM/FORCE PROTECTION DOCUMENTS

DoD Directive 2000.12

DoD Combatting Terrorism Program

DoD Handbook 0-2000.12-H

Protection of DoD Personnel and Activities Against Acts of Terrorism  
and Political Turbulence

DoD Instruction 2000.14

DoD Combating Terrorism Program Procedures

DoD Introduction 0-2000.16

DoD Combating Terrorism Program Standards

GTA 19-4-3

Individual Protective Measures for Personal Security

Joint Pub 3-07.2

Joint Tactics, Techniques, and Procedures for Antiterrorism

AR 190-13

The Army Physical Security Program

AR 190-45

Military Police Law Enforcement Reporting

AR 190-58

Personal Security

AR 195-2

Criminal Investigation Activities

AR 380-19

Information Systems Security

AR 525-13

Antiterrorism Force Protection (AT/FP):  
Security of Personnel, Information and Critical Resources

AR 530-1

Operations Security



# ***Antiterrorism/Force Protection Internet Websites***



## **Department of Defense**

### **Defense LINK Website**

<http://www.dtic.mil/defenselink>

### **DoD Countering Terrorism**

[http://www.defenselink.mil/other\\_info/terrorism.html](http://www.defenselink.mil/other_info/terrorism.html)

### **Defense Information Systems Agency**

<http://www.disa.mil/>

### **DoD Physical Security Equipment Action Group**

<http://www.csc.com/pseag/index.html>

### **Defense Special Weapons Agency**

<http://www.dswa.mil/home.htm>

### **AMC Quick Response Office**

<http://amc.citi.net/amc/qro/>

### **Army Computer Emergency Response Team**

<http://www.acert.belvoir.army.mil/>

### **U.S. Central Command – Force Protection**

<http://www.centcom.mil/antiterrorism/at.htm>



## **Other US Government Sites**

### **USAF Force Protection Battle Lab**

<http://www.fpb.sc.ist.ucf.edu/>

### **Bureau of Alcohol, Tobacco and Firearms**

<http://www.atf.treas.gov/>

### **Central Intelligence Agency**

<http://www.odci.gov/cia/index.html>

### **Department of Justice**

<http://www.usdoj.gov/>

### **Federal Bureau of Investigation**

<http://www.fbi.gov/>

### **Department of State – Travel Information**

<http://travel.state.gov/>

### **Department of State – Countering Terrorism**

<http://www.state.gov/www/global/terrorism/>



# • Purple Heart Medal • AMC Civilian Recipients



|  |
|--|
| <b>Mr. Jim Harry Allen</b><br>13 November 1995<br>PM SANG - Saudi Arabia     |
| Mrs. Sharon K. Batchelder<br>13 November 1995<br>PM SANG - Saudi Arabia      |
| Mrs. Lana P. Breese<br>13 November 1995<br>PM SANG - Saudi Arabia            |
| <b>Mr. Alaric J. Brozovsky</b><br>13 November 1995<br>PM SANG - Saudi Arabia |
| Mr. Jeffrey B. Burbach<br>13 November 1995<br>PM SANG - Saudi Arabia         |
| Mrs. Mary Kay Buschman<br>13 November 1995<br>PM SANG - Saudi Arabia         |
| Mrs. Georgetta R. Combs<br>13 November 1995<br>PM SANG - Saudi Arabia        |
| <b>Mr. William "Dub" Combs</b><br>13 November 1995<br>PM SANG - Saudi Arabia |
| Mr. James A. Coppenger<br>13 November 1995<br>PM SANG - Saudi Arabia         |
| Mrs. Laura R. Croghan<br>13 November 1995<br>PM SANG - Saudi Arabia          |
| Mr. Roland G. Blow<br>25 June 1996<br>MCOM LAR - Saudi Arabia                |

|   |
|---|
| Mrs. Dina Darwish<br>13 November 1995<br>PM SANG - Saudi Arabia           |
| Mrs. Salice L. Edwards<br>13 November 1995<br>PM SANG - Saudi Arabia      |
| Mr. Phillip Florence<br>13 November 1995<br>PM SANG - Saudi Arabia        |
| Mrs. Mary J. Grondin<br>13 November 1995<br>PM SANG - Saudi Arabia        |
| Mrs. Michelle D. Hainsworth<br>13 November 1995<br>PM SANG - Saudi Arabia |
| Ms. Kelli D. Harrison<br>13 November 1995<br>PM SANG - Saudi Arabia       |
| Mrs. Karen A. Heinrich<br>13 November 1995<br>PM SANG - Saudi Arabia      |
| Mr. Tracy V. Henley<br>13 November 1995<br>PM SANG - Saudi Arabia         |
| Mrs. Edna L. Herbka<br>13 November 1995<br>PM SANG - Saudi Arabia         |
| Mr. Curtis L. Holmes<br>13 November 1995<br>PM SANG - Saudi Arabia        |

|   |
|---|
| Mrs. Kathie A. Holt<br>13 November 1995<br>PM SANG - Saudi Arabia   |
| Mrs. Janine B. Hurd<br>13 November 1995<br>PM SANG - Saudi Arabia   |
| Mrs. Beverly A. Jones<br>13 November 1995<br>PM SANG - Saudi Arabia |
| Mrs. Barbara O. Logue<br>13 November 1995<br>PM SANG - Saudi Arabia |
| Mrs. Linda G. Lowry<br>13 November 1995<br>PM SANG - Saudi Arabia   |
| Ms. Niamh L. Miller<br>13 November 1995<br>PM SANG - Saudi Arabia   |
| Mr. Andrew J. Miller<br>13 November 1995<br>PM SANG - Saudi Arabia  |
| Mrs. Cindy L. Moffitt<br>13 November 1995<br>PM SANG - Saudi Arabia |
| Mr. Philip E. Nash<br>13 November 1995<br>PM SANG - Saudi Arabia    |
| Mrs. Sharon W. Rice<br>13 November 1995<br>PM SANG - Saudi Arabia   |

|  |
|--|
| Mrs. Pauline B. Robinson<br>13 November 1995<br>PM SANG - Saudi Arabia       |
| Mrs. Ann M. Russell<br>13 November 1995<br>PM SANG - Saudi Arabia            |
| Mrs. Kathleen S. Schroeder<br>13 November 1995<br>PM SANG - Saudi Arabia     |
| Mr. Walter V. Schwarzhoff<br>13 November 1995<br>PM SANG - Saudi Arabia      |
| Mr. Gregg E. Turner<br>13 November 1995<br>PM SANG - Saudi Arabia            |
| Mr. Bobby J. Ward, Jr.<br>13 November 1995<br>PM SANG - Saudi Arabia         |
| <b>Mr. Wayne Patrick Wiley</b><br>13 November 1995<br>PM SANG - Saudi Arabia |
| Mrs. Susan M. Wood<br>13 November 1995<br>PM SANG - Saudi Arabia             |
| Mr. William R. Wood<br>13 November 1995<br>PM SANG - Saudi Arabia            |
| Mrs. Susan Wright<br>13 November 1995<br>PM SANG - Saudi Arabia              |



# U.S. Army Force Protection Program

*“There is no more important responsibility.”*

General Dennis Reimer

Chief of Staff, U.S. Army

1 November, 1996

*Army Materiel Command*





# AMC Worldwide Presence



**FORCE PROTECTION OFFICE  
HQ, US Army Materiel Command  
5001 Eisenhower Avenue  
Alexandria, VA 22333-0001**

**Commercial: (703) 617-0672  
DSN: 767-0672**